LEGIBILITY NOTICE

A major purpose of the Technical Information Center is to provide the broadest dissemination possible of information contained in DOE's Research and Development Reports to business, industry, the academic community, and federal, state and local governments.

Although a small portion of this report is not reproducible, it is being made available to expedite the availability of information on the research discussed herein.

LA-UR -90-2042

(NNF - 9010121--1

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36

LA-UR--90-2042

DE90 013169

TITLE LAVA/CIS VERSION 2.0: A SOFTWARE SYSTEM FOR VULNERABILITY AND RISK ASSESSMENT

AUTHOR(S) S. T. Smith

SUBMITTED TO 13th National Computer Security Conference, Washington, DC, October 1-4, 1990

DISCLAIMER

Los Alamos National Laboratory
Los Alamos, New Mexico 87545

LAVA/CIS Version 2.0:
A SOFTWARE SYSTEM FOR VULNERABILITY AND RISK ASSESSMENT

S. T. Smith
Safeguards Systems Group, MS-E541
Los Alamos National Laboratory
P. O. Box 1663
Los Alamos, New Mexico 87545

ABSTRACT

LAVA (the Los Alamos Vulnerability/Risk Assessment system) is an original systematic approach to risk assessment developed at the Los Alamos National Laboratory It is an alternative to existing quantitative methods, providing an approach that is both objective and subjective, and producing results that are both quantitative and qualitative. LAVA was developed as a tool to help satisfy federal requirements for periodic vulnerability and risk assessments of a variety of systems and to satisfy the resulting need for an inexpensive, reusable, automated risk assessment tool firmly rooted in science. LAVA is a three-part systematic approach to risk assessment that can be used to model a variety of application systems such as computer security systems, communications security systems, information security systems, and others. The first part of LAVA is the mathematical model based on classical risk assessment, hierarchical multilevel system theory, decision theory, fuzzy possibility theory, expert system theory, utility theory, and cognitive science. The second part is the implementation of the mathematical risk model as a general software engine executed on a large class of personal computers. The third part is the application data sets written for a specific application system. The user of a LAVA application is not required to have knowledge of formal risk assessment techniques. All the technical expertise and specialized knowledge are built into the software engine and the application system itself. LAVA application systems, including the popular computer security application, have been in use by federal government agencies since 1984; the previous computer security version–LAVA/CIS, Version 1.01 [34]–is used by over 100 agencies at more than 500 sites.

INTRODUCTION

LAVA (the Los Alamos Vulnerability/Risk Assessment system) is an original systematic approach to risk assessment developed at the Los Alamos National Laboratory to determine vulnerabilities and risks inherent in massive, complicated systems. Characteristics of such systems are huge bodies of imprecise data, indeterminate (and possibly undetected) events, large quantities of subjective information, and a dearth of objective information. LAVA was developed as a tool to help satisfy federal requirements for periodic vulnerability and risk assessments of a variety of systems and to satisfy the resulting need for an inexpensive, reusable, automated risk assessment tool firmly rooted in science [1]. When the LAVA project began in 1983, there was no such tool [2]; LAVA was designed to fill that gap [3].

LAVA is an alternative to existing quantitative methods, providing an approach that is both objective and subjective, and producing results that are both quantitative and qualitative. In addition, LAVA is used by some agencies as a self-testing aid in preparing for inspections, as a self-evaluating device in testing compliance with the various orders and criteria that exist, and as a certification device by an inspection team.

LAVA is a three-part systematic approach to risk assessment that can be used to model a variety of application systems such as computer security systems, communications security systems, information security systems, and others. The first part of LAVA is the mathematical model based on classical risk assessment [4,5], hierarchical multilevel systems theory [6,7], decision theory [8-10], fuzzy possibility theory [11-15], expert system theory [14,15], utility theory [17,18], and cognitive science [19,20]. (The mathematical model has been presented at other technical meetings [21-23], and generally will not be addressed in depth in this paper.) The second part is the implementation of the mathematical risk model as a general software engine, an expert system framework written in a commercially available programming language for a large class of personal computers. The third part comprises the application data sets written for a specific application system; each application system is a knowledge-based expert system. LAVA provides a framework [24] for creating applications upon which the software engine operates; all application-specific information appears as data.

The user of a LAVA application is not required to have knowledge of formal risk assessment techniques. All the technical expertise and specialized knowledge are built into the software engine and the application system itself. LAVA applications include the popular computer security application [27-30] and applications for nuclear power plant control rooms [31], embedded systems, survivability systems, transborder data flow systems [32], and property control systems. We presently are developing LAVA applications for nuclear processing plant safeguards systems [33] and operations security systems and are discussing the development of a LAVA application for environment, health, and safety issues. LAVA application systems have been in use by federal government agencies since 1984; the previous version–LAVA/CIS, Version 1.01 [34]–is used by over 100 agencies at more than 500 sites.

LAVA/CIS: THE COMPUTER/INFORMATION SECURITY MODEL

The LAVA system was used to develop a hierarchical structure and sets of fuzzy analysis trees for modeling risk assessment for systems associated with computer and information security. Knowledge-based expert systems were built with LAVA to assess risks in application systems comprising a subject system and a safeguards system. The subject system model is sets of threats, assets, and undesirable outcomes; because the threat to security systems is ever-changing, LAVA includes a dynamic threat analysis [25,26]. The safeguards system model has three parts: sets of safeguards functions for protecting the assets from the threats by preventing or ameliorating the undesirable outcomes that may happen to the assets, sets of safeguards subfunctions whose performance determine whether the function is adequate and complete, and sets of issues, appearing in the software as interactive questionnaires, whose measures (in both monetary and linguistic terms) define both the weaknesses in the safeguards system and the potential costs of an undesirable outcome occurring as a result of a successful attack against safeguards system weaknesses.

For the computer/information security application model, LAVA/CIS, the set of postulated assets consists of four categories: (1) the facility, including physical plant and personnel; (2) hardware, including all computing and ancillary pre- and postprocessing hardware; (3) machine-interpretable information, including software, input and output files, and databases; and (4) human-interpretable information, including documents, screen displays, graphs, charts, film output, and so forth. The model's threat set consists of three categories: (1) natural, random, and environmental hazards; (2) direct or onsite humans, including the authorized insider; and (3) indirect or offsite humans (but this threat category has not yet been implemented in the software). Figures 1 and 2 show the hierarchical structures for the three threat categories with respect to the four asset categories. Included as the third and fourth levels in these hierarchies, and discussed later in this paper, are representative safeguards functions and subfunctions associated with each threat-asset pair; Fig. 3 shows the complete analysis structure for the [direct human threat, software asset] combination.

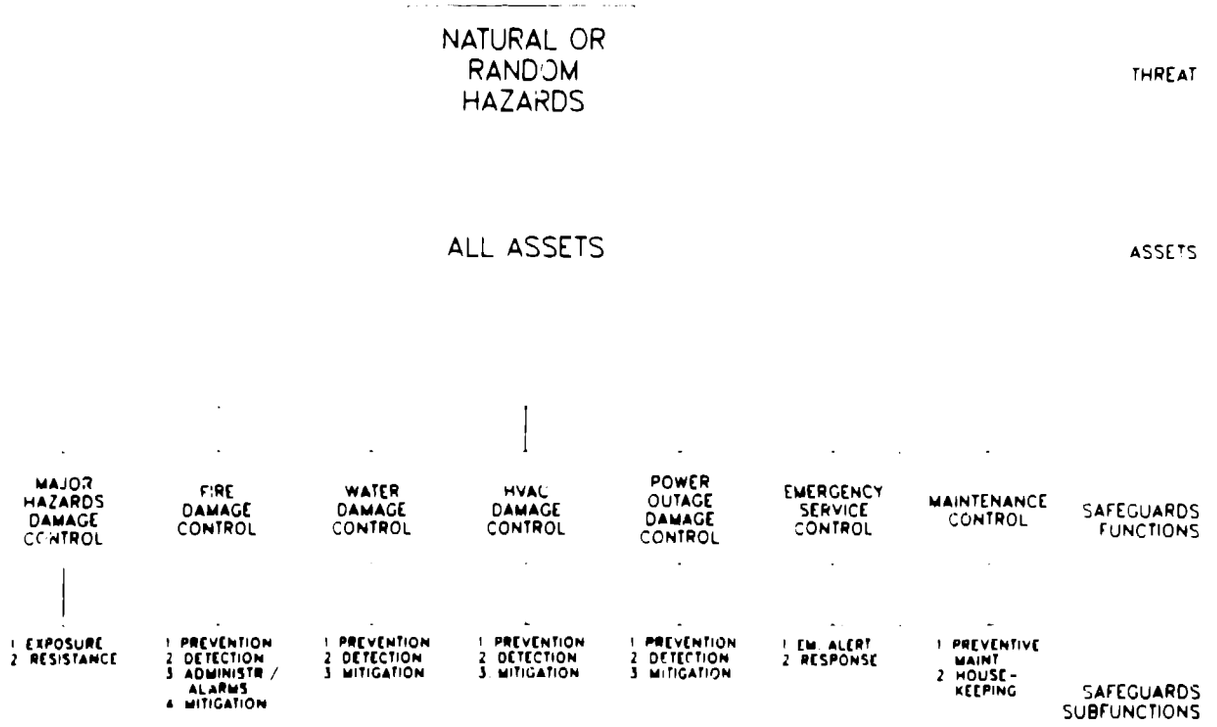
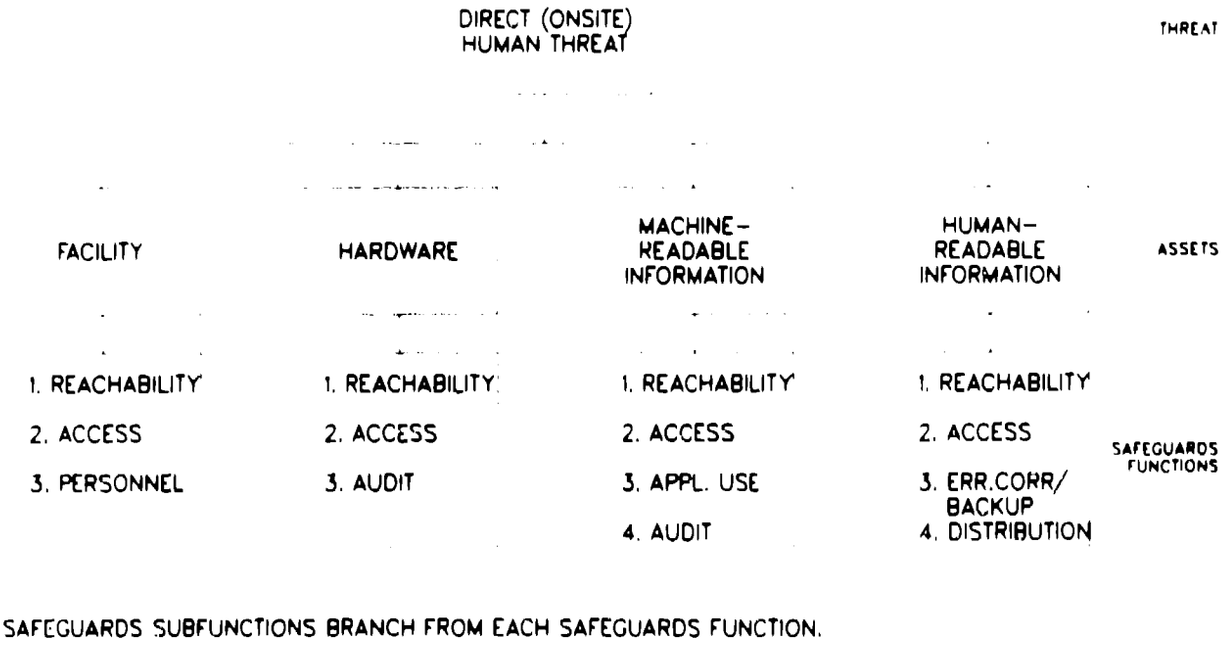


Fig. 1. Natural Hazards Hierarchy for Computer/Information Security Application



SAFEGUARDS SUBFUNCTIONS BRANCH FROM EACH SAFEGUARDS FUNCTION.

Fig. 2. Direct (Onsite) Human Threat Hierarchy for Computer/Information Security Application

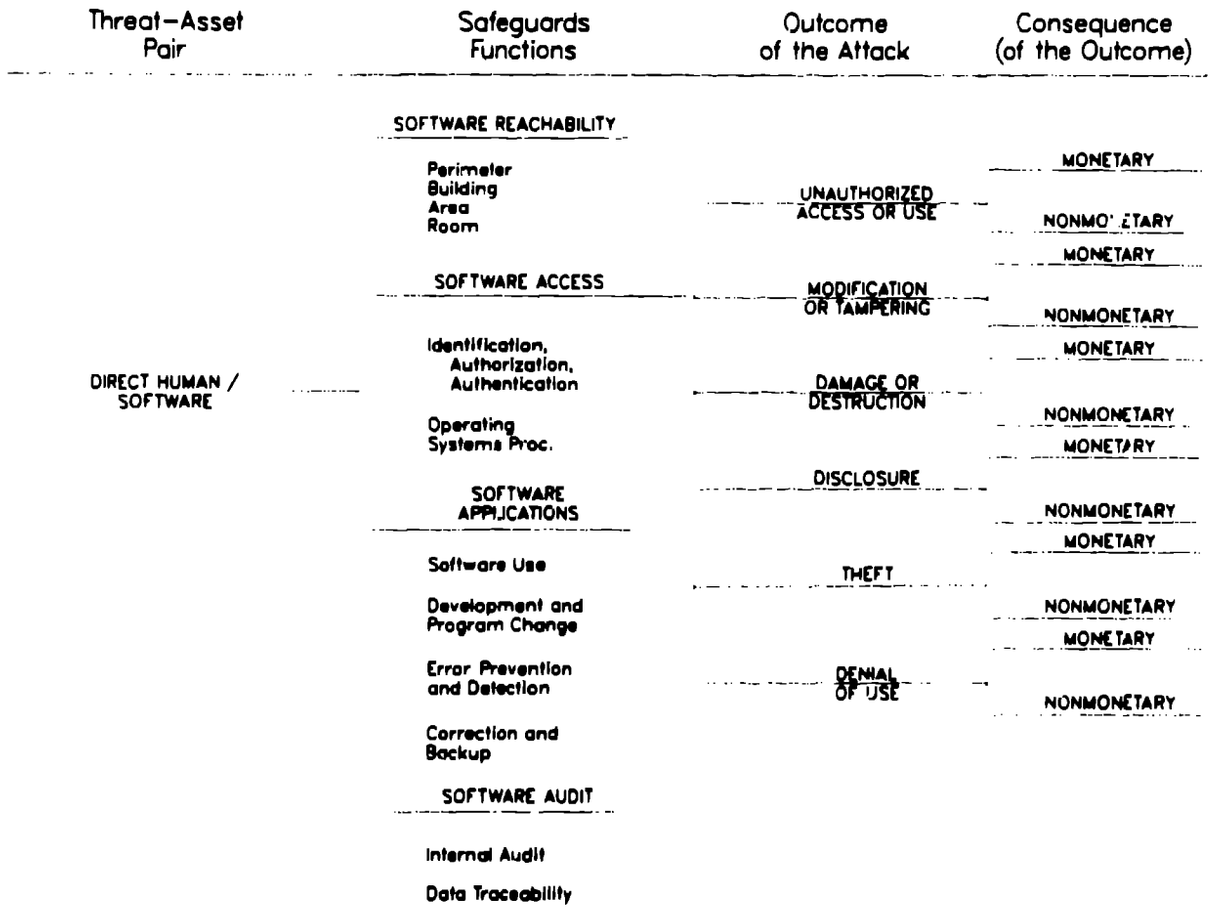


Fig. 3. Direct Human-Software Scenario Analysis Tree for Computer/InformationSecurity Application

Six undesirable outcomes are considered in the computer/information security model: (1) unauthorized access or use; (2) damage, modification, or tampering; (3) destruction; (4) theft; (5) unauthorized disclosure; and (6) denial of use. It is important to note that a single event can result in the simultaneous occurrence of more than one of the outcomes. Figure 4 shows the outcome possibility matrix for the threat-asset combinations; a value of zero indicates that the outcome is impossible for that threat-asset combination, and a value of one means the outcome is possible for that threat-asset pair; greater granularity can be achieved by assigning values lying between zero and one, indicating varying degrees of possibility for the occurrence of each outcome.

The ideal safeguards system prevents the threats from attacking the assets and achieving the postulated outcomes. The safeguards system model consists of a set of safeguards functions for each of the distinguishable threat-asset pairs (nine T-A pairs, in this application) in such a way that the relative importance of each function within the set of functions for each T-A pair is about the same. Then, for each of the individual safeguards functions, a set of subfunctions provides performance criteria for the adequacy and completeness of that safeguards function; each of the subfunctions is devised so that the relative importance of each subfunction within a specific function is about the same. Again referring to Figs. 1-3, the figures show the safeguards functions and subfunctions for each distinguishable threat-asset pair.

	Unauthorized Access or Use	Modification or Tampering	Damage or Destruction	Disclosure	Theft	Denial of use
Natural Hazards – Facility	0	1	1	0	0	1
Natural Hazards – Hardware	0	1	1	0	0	1
Natural Hazards – Software	0	1	1	0	0	1
Natural Hazards – Documents/ Displays	0	1	1	0	0	1
Direct Human – Facility	1	1	1	1	1	1
Direct Human – Hardware	1	1	1	1	1	1
Direct Human – Software	1	1	1	1	1	1
Direct Human – Documents/ Displays	1	1	1	1	1	1

Fig. 4. Outcome Possibility Matrix for Computer/Information Security Application

LAVA evaluates the value of the assets to the organization in qualitative terms. The evaluation takes into account the criticality of the asset to organizational operations, the sensitivity of the asset to adversarial gain from theft or disclosure, and the necessity for the asset to maintain its integrity in terms of modification. The user may also specify monetary values for the asset to maintain its integrity in terms of modification. The user may also specify monetary values for the assets in any consistent currency system (LAVA's expertise does not extend to currency conversion).

Both government and corporate organizations may be the targets of a variety of hostile agents [35,36], and the intensity of the threat may change with time and circumstances. The dynamic threat strength can be analyzed if the subject system is extremely sensitive to a changing threat and if the subject organization has access to the kinds of information the analysis requires. The dynamic threat analysis takes into account possible threat agents and their potential attack goals with respect to the target(s) of the attack. The dynamic aspects of the natural hazards may or may not be of interest; these include both random natural hazards, such as volcanic eruptions or earthquakes, as well as the natural hazards more cyclic in nature, such as hurricanes, tornadoes, torrential rains, and the like. The human threat agents in each of the human threat categories all act for different reasons, so they may differ widely in motivation, capability, and opportunity. Similarly, the goals of the attacks may vary, but all categories of goals may be used by all categories of threat agents. Clearly, more than one of the goal categories may be the goal of a single attack, and a single attack may be perpetrated by more than one category of threat agent. Figure 5 illustrates the dynamic threat analysis structures. A more detailed discussion of the dynamic threat analysis can be found in References 25 and 26.

The impact analysis measures costs in both qualitative and quantitative terms: LAVA uses qualitative measures for intangible cost sources like loss of reputation or strategic posture, and quantitative measures for tangibles like repair/replacement costs or litigation costs.

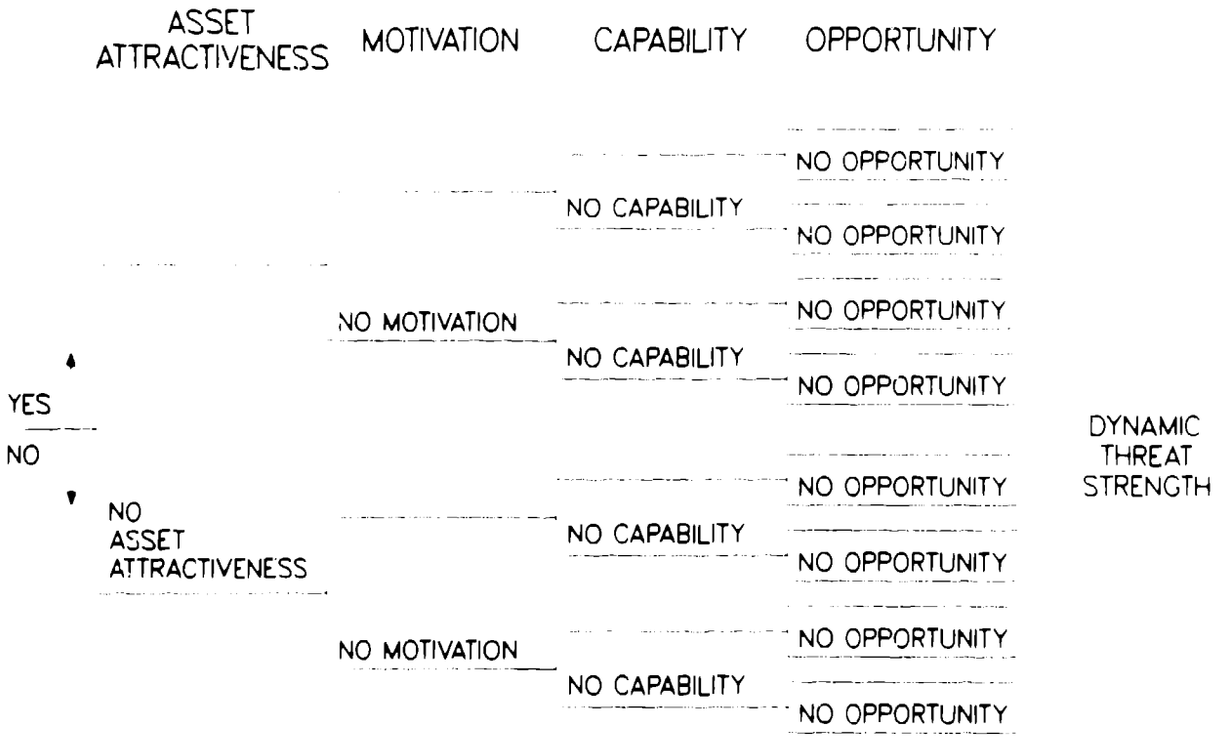


Fig. 5. Analysis Structure for Dynamic Threat

Loss exposure, or risk, results from a combination of asset value, threat strength, safeguards system weakness, and event costs. LAVA calculates both a monetary and a nonmonetary loss exposure measure for each [threat, asset, safeguards function, outcome, impact] combination. These loss exposure values can be aggregated in whatever ways are of interest to the user; less aggregation provides more information for specific decision making, but more aggregation provides a bottom line for upper management..

FEATURES OF LAVA/CIS VERSION 2.0

The long-awaited new version of the computer and risk assessment application of LAVA, LAVA/CIS Version 2.0, was released for the first time on a limited basis in April 1990. The new version has a much improved vulnerability assessment section, and has the additions of an asset-value estimation, a threat-strength estimation, and both monetary and nonmonetary (or intangible) impact analysis, expanding the LAVA 2.0 software engine into a full risk assessment package. This section discusses what the software is, what its operating requirements are, and how it is distributed.

What is LAVA 2.0 and what are its operating requirements? The LAVA 2.0 general software engine is a compiled, fully self-contained piece of software that runs on the IBM-PC class of personal computers. No additional software other than MS- or PC-DOS (version 2.0 or greater) is required to run LAVA 2.0. Minimum required hardware includes 1) 512 K available random-access memory, 2) a hard disk with about 1 megabyte of available space to store LAVA.EXE and the permanent application data sets, and 3) a floppy disk drive for the diskette holding the volatile application data sets. The report generators are compatible with a wide variety of dot-matrix, ink-jet, and laser printers.

What is new about LAVA/CIS 2.0? Instead of multiple code segments, LAVA 2.0 is integrated into a single menu-driven program; the menu items are selected with user-friendly light bars. Like previous versions, LAVA 2.0 applications are completely self-documented. In addition to the many definition and instruction screens, the LAVA 2.0 software engine now can display specific definitions selected as needed by the user during the progress of a LAVA assessment.

Besides an updated, much-improved vulnerability assessment (VA) portion, the new version includes a consequence analysis (CA) portion, making LAVA 2.0 a full risk assessment software system. The CA portion comprises an asset-value estimation, a threat-strength estimation, an outcome-severity mitigation estimation, and both monetary and nonmonetary (or intangible) impact analysis. The interactive vulnerability and consequence analysis questionnaire segments have hot keys for backing up in the questionnaire and for making a graceful emergency exit from the questionnaire if necessary. Both the VA and CA sections have independent report generators; the VA report format is fixed but has user-selectable graphic displays, and the entire CA format can be tailored by the user. The VA interactive, scoring, and reporting segments can be executed without doing the CA section. The interactive portion of the CA can be executed before, after, or at the same time as the VA; however, the CA scoring and reporting segments can not be run until after the VA has been completed.

In addition, a set of utility options permits the user to print unanswered questionnaires, partially answered questionnaires as memory refreshers in mid-assessment, fully-answered questionnaires at the completion of the VA for documentation purposes, and management worksheets for issue resolution. Finally, the LAVA 2.0 software engine now has color capabilities for those who have color monitors.

The data sets for LAVA/CIS Version 2.0 have been modified and expanded over those of Version 1.01. Some additional issues have been considered in the VA questionnaires, the security-requirement determination has been modified slightly, the underlying outcome set has been changed a little, and many of the VA questions have had their wording clarified. The definition screens have been reorganized so that there is only one definition per screen. All data sets for the CA portion are new.

All in all, the new LAVA 2.0 software engi is chock full of new features, all designed with the user in mind. Upgrading to the new computer- and information-security application, LAVA/CIS Version 2.0, should be very worthwhile!

How does one obtain LAVA/CIS? The Los Alamos National Laboratory is distributing the LAVA Software System for Computer and Information Security, LAVA/CIS Version 2.0, free of charge to Government agencies. It is available only to graduates of a LAVA training workshop–those who have faithfully attended and participated in the workshop. Because the workshops are an unfunded activity, there is a fee for the training workshops to recover workshop costs.

LAVA Workshops at Los Alamos and elsewhere. The LAVA/CIS Version 2.0 workshops, usually held at Los Alamos, last a full five days from 8:30 a.m. to 5:00 p.m. daily. The workshops present the LAVA philosophy and mathematical approach to vulnerability and risk assessment, and are hands-on workshops in which the participants complete a real assessment of a real computer installation. Attendance at all class sessions is required to graduate and receive the LAVA/CIS 2.0 software that is distributed to the graduates at the end of the workshop.

The workshops are intended for persons who have the responsibility for vulnerability and risk assessments in the computer- and information-security area; persons who require training in physical, technical, informational, and operations security activities; security auditors; and persons who manage security activities. The instruction staff provides help in how to use LAVA/CIS for vulnerability and risk assessments, as a training aid, as a preparation for security audits and compliance inspections, as a design tool, and as a decision aid.

If an agency wishes, the LAVA staff can hold a workshop/assessment at a site specified by the agency. The basic workshop content would be the same as those held at Los Alamos, but the agency could have as many participants as desired, and the workshop would produce a valid assessment of an installation belonging to the agency.

CONCLUSIONS

LAVA/CIS Version 2.0 is a comprehensive, rigorous, understandable approach to computer/information security risk assessment. It is a very affordable alternative to high-priced commercial risk assessment software. It can be used in-house by agency employees, obviating the need for the expensive services of outside consultants. Its flexibility in the order of execution of its various parts, in doing a stand-alone vulnerability assessment or a complete risk assessment, in doing either only nonmonetary impact analysis or both monetary and nonmonetary impact analysis, and in tailoring its reports contributes to its ease of use.

In addition, LAVA's capability to assess the dynamic aspects of the threat spectrum makes it an ideal tool for modelling applications of interest to the intelligence and military communities. It would also be highly applicable in the business community in situations ripe for industrial espionage.

Using the LAVA approach for risk assessment has benefits that do not accrue from the use of other methods. First, the automated report generators produce results that are immediately usable, both to managers who must make major, far-reaching decisions and to the security personnel in the field whose job it is to maintain an acceptable level of safeguards. Second, because LAVA produces both qualitative and quantitative results, users feel more comfortable with the results because they understand both the results and the information that produced those results. Third, because LAVA does not require the user to generate probabilities (often unfounded) for its operation but instead relies on a natural-language user-friendly interface to acquire its data, users are more willing to act upon its results. Fourth, LAVA includes a way to assess the changing, or dynamic, aspects of the threat spectrum. And finally, because of the team environment in which an assessment is performed and the discussions that arise among team members, using a LAVA application has proved to be an experience that both raises the security consciousness of the users and enhances the overall working environment at the facility.

REFERENCES

1. S. Katzke, "National Bureau of Standards Perspective on Risk Analysis: Past, Present, and Future," presented at the 1st Federal Risk Analysis Workshop, Montgomery, Alabama, January 1985.

2. S. T. Smith, "A Government-Wide Overview of Risk Analysis Methodologies," presented at the 8th DOE Computer Security Group Conference, Richland, Washington, April 1985.

3. S. T. Smith and J. J. Lim, "An Automated Procedure for Performing Computer Security Risk Analysis," in Proceedings 6th Annual ESARDA Symposium on Safeguards and Nuclear Material Management, May 1984, pp. 527-530.

4. N. J. McCormick, Reliability and Risk Analysis Methods and Nuclear Power Applications. New York: Academic Press, 1981.

5. W. D. Rowe, An Anatomy of Risk. New York: John Wiley & Sons, 1977.

6. M. D. Mesarovic, D. Macks, and Y. Takahara, Theory of Hierarchical Multilevel Systems. New York and London: Academic Press, 1970.

7. Y. M. I. Dirickx and L. P. Jennergren, Systems Analysis by Multilevel Methods. New York: John Wiley & Sons, 1979, pp. 10-82.

8. P. C. Fishburn, Decision and Value Theory. New York: John Wiley & Sons, 1964.

9. R. L. Keeney and H. Raiffa, Decisions with Multiple Objectives: Preferences and Value Tradeoffs. New York: John Wiley & Sons, 1976.

10. R. Schlaifer, Analysis of Decisions Under Uncertainty. Huntington, New York: Robert E. Krieger Publishing Company, 1978.

11. R. E. Bellman and L. A. Zadeh, "Decision-making in a Fuzzy Environment," Management Science, Vol. 17, No. 4, December 1970.

12. A. Kaufmann and M. M. Gupta, Introduction to Fuzzy Arithmetic: Theory and Applications. New York: Van Nostrand Reinhold Company, 1985.

13. L. A. Zadeh, "Fuzzy Sets as a Basis for a Theory of Possibility," Fuzzy Sets and Systems, Vol. 1, pp. 3-28, 1978.

14. C. V. Negoita, Expert Systems and Fuzzy Systems. Menlo Park, California: The Benjamin/ Cummings Publishing Company, Inc., 1985, pp. 52-58, 74-88, 95-112.

15. P. H. Winston, Artificial Intelligence. Reading, MA: Addison-Wesley, 1984, pp. 251-288.

16. R. Jain, "A Procedure for Multiple-Aspect Decision-Making Using Fuzzy Sets," Int. J. Systems Sci., Vol. 8, No. 1, pp. 1-7, January 1977.

17. P. J. H. Schoemaker and C. C. Waid, "An Experimental Comparison of Different Approaches to Determining Weights in Additive Utility Models," Management Science, Vol. 28, No. 2, February 1982.

18. E. M. Johnson and G. P. Huber, "The Technology of Utility Assessment," IEEE Trans. Sys., Man, Cyber., Vol. SMC-7, No. 5, May 1977.

19. L. A. Zadeh, K.-S. Fu, K. Tanaka, and M. Shimura (Eds.), Fuzzy Sets and their Applications to Cognitive and Decision Processes. New York: Academic Press, 1975.

20. S. Sudman and N. M. Bradburn, Asking Questions: A Practical Guide to Questionnaire Design. San Francisco: Jossey-Bass, Inc., 1982.

21. S. T. Smith and J. J. Lim, "An Automated Interactive Expert System for Evaluating the Effectiveness of Computer Security Measures, presentyed at the 7th Department of Defense/National Bureau of Standards Computer Security Conference, Gaithersburg, Maryland, September 24-27, 1984.

22. S. T. Smith, J. R. Phillips, R. M. Tisinger, J. J. Lim, D. C. Brown, and P. D. FitzGerald, "LAVA: A Conceptual Framework for Automated Risk Analysis," presented at the 1986 Annual Meeting of the Society for Risk Analysis, Boston, Massachusetts, November 9-12, 1986.

23. S. T. Smith, "LAVA: An Expert System Framework for Risk Analysis," presented at the 1st International Computer Security Risk Management Model Builders Workshop, Denver, Colorado, May 24-26, 1988.

24. S. T Smith and J. J. Lim, "Framework for Generating Expert Systems to Perform Computer Security Risk Analysis," in Proceedings First Annual Armed Forces Communications and Electronics Association Symposium and Exposition on Physical and Electronics Security, August 1985, pp. 24-1–24-7.

25. S. T. Smith, J. R. Phillips, D. C. Brown, and P. D. FitzGerald, "Assessing the Threat Component for the LAVA Risk Management Methodology," in Proceedings 9th DOE Computer Security Group Conference, May 1986, pp.118-123.

26. S. T. Smith, "Risk Assessment and LAVA's Dynamic Threat Analysis," in Proceedings 12th National Computer Security Conference, October 1989, pp. 483-494.

27. S. T. Smith and J. J. Lim, "An Automated Method for Analyzing Computer Security Risk," presented at the 7th DOE Computer Security Group Conference, New Orleans, Louisiana, April 10-12, 1984.

28. S. T. Smith and J. J. Lim, "An Automated Method for Assessing the Effectiveness of Computer Security Safeguards," in Proceedings IFIPS Second International Congress on Computer Security, Toronto, Canada, September 1984.

29. S. T. Smith and J. J. Lim, "LAVA: An Automated Computer Security Vulnerability Assessment Software System (Version 0.9)," Los Alamos National Laboratory document LA-UR-85-4014, December 1985.

30. S. T. Smith et al., "LAVA for Computer Security: An Application of the Los Alamos Vulnerability Assessment Methodology," Los Alamos National Laboratory document LA-UR-86-2942, 1986.

31. S. T. Smith and J. J. Lim, "Assessment of Computer Security Effectiveness for Safe Plant Operation," Trans. Am. Nucl. Soc., Vol. 46, pp. 525-526, 1984.

32. S. T. Smith, J. J. Lim, and J. Lobel, "Application of Risk Assessment Methodology to Transborder Data Flow,"in Handbook on the International Information Economy, Transnational Data Report, Springfield, VA (November 1985).

33. S. T. Smith and R. M. Tisinger, "Modeling Risk Assessment for Nuclear Processing Plants with LAVA," Nucl. Mater. Manage., Vol. XVII, pp. 101-104, 1988.

34. S. T. Smith et al., "LAVA for Computer Security: An Application of the Los Alamos Vulnerability Assessment Methodology, Release Version 1.01," Los Alamos National Laboratory document LA-UR-86-2942,September 1987.

35. N. R. Bottom, Jr., and R. R. J. Gallati, Industrial Espionage: Intelligence Techniques and Countermeasures. Boston: Butterworth Publishers, 1984.

36. R. Eells and P. Nehemkis, Corporate Intelligence and Espionage: A Blueprint for Executive Decision Making. New York: Macmillan, 1984.